#7 DFW

Attorney Docket No. 36321-8009.US01

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

Date: 8-4-06 By: Susan L. Baka

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: BONEH ET AL.	EXAMINER: BAO TRAN N TO
APPLICATION NO.: 10/038,169	ART UNIT: 2135
FILED: January 2, 2002	CONFIRMATION NO: 7811
FOR: METHOD AND APPARATUS FOR TRANSPARENT TRANSCRIPTION	

Information Disclosure Statement Within Three Months of Application Filing or Before First Action – 37 C.F.R. § 1.97(b)

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The undersigned submits the following references without admitting that any enclosed item of information constitutes prior art to the subject invention and specifically reserves the right to demonstrate that any such reference is not prior art. The undersigned, in an effort to focus the scope of this review, has identified the following subsets of references as most relevant to the subject invention:

U.S. PATENT DOCUMENTS

Cite No.	U.S. Patent/Appln. Number	Name of Patentee or Inventor	Filing/Publication /Issue Date
1.	5,828,832	Holden et al.	10/27/1998
2.	6,073,242	Hardy et al.	6/6/2000
3.	6,098,096	Tsirigotis et al.	8/1/2000
4.	6,216,212	Challenger et al.	4/10/2001
5.	6,233,577	Ramasubramani et al.	5/15/2001

6.	6,397,330	Elgamal et al.	5/28/2002
7.	6,519,365	Kondo et al.	2/11/2003
8.	6,678,733	Brown et al.	1/13/2004
9.	6,941,459	Hind et al.	9/6/2005
10.	6,963,980	Mattsson	11/5/2005
11.	6,990,636	Beauchamp	1/24/2006
12.	11/236,046	Metzger et al.	9/26/05
13.	11/236,061	Metzger et al.	9/26/05
14.	11/341,060	Metzger et al.	1/2706
15.	2002/0016911	Chawla et al.	2/7/2002
16.	2003/0123671	He at al.	7/3/2003
17.	2003/0156719	Cronce	8/21/2003
18.	2006/0041533	Koyfman 8032.US01	2/23/2006
19.	2006/0149962	Fountain et al.	7/6/2006

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

Cite No.	
20.	Boneh, et al., "Efficient Generation of Shared RSA Keys," (extended abstract)
21.	Menezes, A., et al., "Handbook of Applied Cryptography," 1996 CRC Press, pp. §8.2-8.3 and §14.5
22.	RSA "PKCS #1 v2.0 Amendment 1: Multi-Prime RSA," 2000
23.	Shand, M., et al., "Fast Implementations of RSA Cryptography," 1993
24.	Stallings, W., "IP Security," Network Security Essentials, Applications and Standards, Chapters 6 and 7, pp. 162-223, 2000
25.	Takagi, T., "Fast RSA-Type Cryptosystem Modulo $p^k q$," 1998
26.	Takagi, T., "Fast RSA-Type Cryptosystems Using N-Adic Expansion," Advances in Technology – CRYPTO '97, LNCS 1294, pp. 372-384, 1997

1. Timing of Submission

This information disclosure is being filed within three months of the filing date of this application or date of entry into the National Stage of an International Application or before the mailing date of a first Office Action on the merits or before the mailing date of a first Office Action on the merits after the filing of a Request for Continued Examination under 37 CFR §1.114, whichever occurs last (37 CFR 1.97(b)(4)). The references listed on the enclosed Form PTO-1449 (modified) may be material to the examination of this application; the Examiner is requested to make them of record in the application.

2. Cited Information

☒ Copies of the following references are enclosed:

- ☐ All cited references
- ☐ References marked by asterisks
- ☒ The following: References A44 through A48, B1, B2 and C1 through C24.

3. Effect of Information Disclosure Statement (37 C.F.R. § 1.97(h))

This Information Disclosure Statement is not to be construed as a representation that: (i) a search has been made; (ii) additional information material to the examination of this application does not exist; (iii) the information, protocols, results and the like reported by third parties are accurate or enabling; or (iv) the cited information is, or is considered to be, material to patentability. In addition, applicant does not admit that any enclosed item of information constitutes prior art to the subject invention and specifically reserves the right to demonstrate that any such reference is not prior art.

4. Fee Payment

No fees are believed due because this Information Disclosure Statement is being filed before the mailing date of the first Office Action.

However, should the Commissioner determine that fees are due in order for this Information Disclosure Statement to be considered, the Commissioner is hereby authorized to charge such fees to Deposit Account No. 50-2207.

5. Patent Term Adjustment (37 C.F.R. § 1.704(d))

☐ The undersigned states that each item of information submitted herewith was cited in a communication from a foreign patent office in a counterpart

application and that this communication was not received by any individual designated in 37 C.F.R. § 1.56(c) more than thirty days prior to the filing of this statement. 37 C.F.R. § 1.704(d).

Respectfully submitted,
Perkins Coie LLP

Date: August 4, 2006

William F. Ahmann
Registration No. 52,548

Correspondence Address:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, California 94026
(650) 838-4300

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
Form PTO-1449 (Modified)
(Use several sheets if necessary)

Sheet	1	of	6

COMPLETE IF KNOWN	
Application Number	10/038,169
Confirmation Number	7811
Filing Date	January 2, 2002
First Named Inventor	Boneh
Group Art Unit	2135
Examiner Name	Bao Tran N To
Attorney Docket No.	36321-8009.US01

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	U.S. Patent or Application NUMBER	Kind Code (if known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1.	4,386,416		Giltner	5/31/1983	
	A2.	4,964,164		Fiat, Amos	10/16/1990	
	A3.	5,222,133		Chou et al.	6/22/1993	
	A4.	5,557,712		Guay	9/17/1996	
	A5.	5,734,744		Wittenstein	3/31/1998	
	A6.	5,764,235		Hunt et al.	6/9/1998	
	A7.	5,828,832		Holden et al.	10/27/1998	
	A8.	5,848,159		Collins et al.	12/8/1998	
	A9.	6,021,198		Anigbogu	2/1/2000	
	A10.	6,073,242		Hardy et al.	6/6/2000	
	A11.	6,081,598		Dai, Wei	6/27/2000	
	A12.	6,081,900		Subramaniam et al.	6/27/2000	
	A13.	6,094,485		Weinstein, et al.	7/25/2000	
	A14.	6,098,093		Bayeh et al.	8/1/2000	
	A15.	6,098,096		Tsirigotis et al.	8/1/2000	
	A16.	6,154,542		Crandall	11/28/2000	
	A17.	6,202,157		Brownlie et al.	3/13/201	
	A18.	6,216,212		Challenger et al.	4/10/2001	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
				Examiner Name	Bao Tran N To
Sheet	2	of	6	Attorney Docket No.	36321-8009.US01

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.	U.S. Patent or Application NUMBER	Kind Code (if known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A19.	6,233,577		Ramasubramani et al.	5/15/2001	
	A20.	6,396,926		Takagi, et al.	5/28/2002	
	A21.	6,397,330		Elgamal et al.	5/28/2002	
	A22.	6,473,802		Masters	10/29/2002	
	A23.	6,477,646		Krishna, et al.	11/5/2002	
	A24.	6,502,135		Munger et al.	12/31/2002	
	A25.	6,519,365		Kondo et al.	2/11/2003	
	A26.	6,578,061		Aoki, et al.	6/10/2003	
	A27.	6,584,567		Bellwood et al.	6/24/2003	
	A28.	6,587,866		Modi et al.	7/1/2003	
	A29.	6,615,276		Mastrianni et al.	9/2/2003	
	A30.	6,621,505		Beauchamp et al.	9/16/2003	
	A31.	6,678,733		Brown et al.	1/13/2004	
	A32.	6,681,327		Jardin, Cary A.	1/20/2004	
	A33.	6,694,323		Bumbulis	2/17/2004	
	A34.	6,751,677		Ilkicki et al.	6/15/2004	
	A35.	6,757,823		Rao et al.	6/29/2004	
	A36.	6,763,459		Corella, Francisco	7/13/2004	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
				Examiner Name	Bao Tran N To
Sheet	3	of	6	Attorney Docket No.	36321-8009.US01

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	U.S. Patent or Application NUMBER	Kind Code (if known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A37.	6,874,089		Dick et al.	3/29/2005	
	A38.	6,886,095		Hind et al.	4/26/2005	
	A39.	6,915,427		Maruyama et al.	7/5/2005	
	A40.	6,941,459		Hind et al.	9/6/2005	
	A41.	6,963,980		Mattsson	11/5/2005	
	A42.	6,990,636		Beauchamp	1/24/2006	
	A43.	6,990,660		Moshir et al.	1/24/2006	
	A44.	10/526,252		Fountain et al. 8024	2/24/2005	
	A45.	11/236,046		Metzger et al. 8033	9/26/2005	
	A46.	11/236,061		Metzger et al. 8035	9/26/2005	
	A47.	11/236,294		Metzger et al. 8034	9/26/2005	
	A48.	11/341,060		Metzger et al. 8036	1/27/06	
	A49.	2002/0016911		Chawla et al.	2/7/2002	
	A50.	2002/0039420		Schacham et al.	4/4/2002	
	A51.	2002/0066038		Mattsson	5/30/2002	
	A52.	2002/0073232		Hong et al.	6/13/2002	
	A53.	2002/0087884		Schacham et al.	7/4/2002	
	A54.	2003/0014650		Freed et al.	1/16/2003	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
				Examiner Name	Bao Tran N To
Sheet	4	of	6	Attorney Docket No.	36321-8009.US01

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	U.S. Patent or Application NUMBER	Kind Code (if known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A55.	2003/0065919		Albert et al.	4/3/2003	
	A56.	2003/0097428		Afkhami	5/22/2003	
	A57.	2003/0101355		Mattsson	5/29/2003	
	A58.	2003/0123671		He at al.	7/3/2003	
	A59.	2003/0156719		Cronce	8/21/2003	
	A60.	2004/0015725		Boneh et al.	1/22/2004	
	A61.	2006/0041533		Koyfman	2/23/2006	
	A62.	2006/0149962		Fountain et al.	7/6/2006	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.	Foreign Patent or Application Office	NUMBER	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
	B1.	WO	01/03398		IBM Corp and IBM UK Limited	01/11/2001		
	B2.	WO	02/101605		Research In Motion Limited	12/19/02		

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
	C1.	Alteon Web Systems: "The Next Step in Server Loading Balancing" November 1999, Retrieved from the Internet: URL:http:/www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf, Retrieved on March 2, 2004; pages 4-11.	
	C2.	Alteon Web Systems: "Networking with the Web in Mind" May 1999, Retrieved from the Internet: URL:http:/www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf, Retrieved on March 2, 2004; page 1, pages 3-7.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
				Examiner Name	Bao Tran N To
Sheet	5	of	6	Attorney Docket No.	36321-8009.US01

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
	C3.	Boneh, D., "Twenty Years of Attacks on the RSA Cyrptosystem," Notices of the AMS, Vol 46, No. 2, pp. 203-213, 1999	
	C4.	Boneh, et al., "An Attack on RSA Given a Small Fraction of the Private Key Bits," ASIACRYPT '98, LNCS 1514, pp. 25-34, 1998	
	C5.	Boneh, et al., "Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$," (extended abstract), 1999	
	C6.	Boneh, et al., "Efficient Generation of Shared RSA Keys," (extended abstract)	
	C7.	Durfee, G., et al., "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99," ASIACRYPT 2000, LNCS 1976, pp. 14-29, 2000	
	C8.	Fiat, A. "Batch RSA, (digital signatures and public key krypto-systems)" Advances in Crytology – Cryto '89 Proceedings 20-24 August, 1989, Springer-Verlag	
	C9.	Großschädl, J., et al., "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip," 2000	
	C10.	Herda, S., "Non-repudiation: Constituting evidence and proof in digital cooperation," Computer Standards and Interfaces, Elsevier Sequoia, Lausanne, CH, 17:1 (69-79) 1995.	
	C11.	Immerman, N., "Homework 4 with Extensive Hints," 2000	
	C12.	Menezes, A., et al., "Handbook of Applied Cryptography," 1996 CRC Press, pp. §8.2-8.3 and §14.5	
	C13.	Netscape; "Netscape Proxy Server Administrator's Guide, Version 3.5 for Unix"; February 25, 1998; Retrieved from the Internet.	
	C14.	Oppliger, R.; "Authorization Methods for E-Commerce Applications"; 1999	
	C15.	RSA Laboratories: "PKCS #7: Cryptographic Message Syntax Standard, Version 1.5," RSA Laboratories Technical Note, pp. 1-30, November 1, 1993.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).

/ 0

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
				Examiner Name	Bao Tran N To
Sheet	6	of	6	Attorney Docket No.	36321-8009.US01

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
	C16.	RSA "PKCS #1 v2.0 Amendment 1: Multi-Prime RSA," 2000	
	C17.	"Security Protocols Overview (An RSA Data Security Brief)", RSA Data Security, 1999, http://www.comms.scitech.susx.ac.uk/fft/crypto/security_protocols.pdf, pages 1-4.	
	C18.	Schacham, H., et al., "Improving SSL Handsake Performance via Batching," Topics in Cryptology, pp. 28-43, 2001.	
	C19.	Shand, M., et al., "Fast Implementations of RSA Cryptography," 1993	
	C20.	Sherif, M.H., et al., "SET and SSL: Electronic Payments on the Internet," IEEE, pp. 353-358 (1998)	
	C21.	Stallings, W., "IP Security," Network Security Essentials, Applications and Standards, Chapters 6 and 7, pp. 162-223, 2000	
	C22.	Takagi, T., "Fast RSA-Type Cryptosystem Modulo $p^k q$," 1998	
	C23.	Takagi, T., "Fast RSA-Type Cryptosystems Using N-Adic Expansion," Advances in Technology – CRYPTO '97, LNCS 1294, pp. 372-384, 1997	
	C24.	Wiener, M., "Cryptanalysis of Short RSA Secret Exponents," 1989	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).